

REMARKS

Applicants have thoroughly considered the Examiner's remarks in the June 11, 2009 Office action and have amended the application to more clearly set forth aspects of the claims. Claims 1, 4–7, 10–13, 16, 17, 19–24, 27, 28, 30, 31, and 36–41 are presented in the application for further examination. Claims 1, 6, 7, 10–13, 23, 24, 27, 28, 30, and 38 have been amended by this Amendment C. Reconsideration of the application claims as amended and in view of the following remarks is respectfully requested.

Interview Summary

Applicants thank the Examiner for the courtesy of a telephonic interview on April 23, 2009. Applicants communicated distinguishing aspects of the claims over the cited reference – for example, Traversat teaches away from providing from a centralized location access control to a resource for one or more users, by disclosing instead distributed, decentralized methods of providing peer group services on a peer-to-peer network. No formal agreement was reached. This Amendment C reflects the discussion during the interview.

Drawings

Applicants again respectfully request that the Examiner now have the drawings as originally filed reviewed and accepted.

Claim Rejections under 35 U.S.C. § 103

Claims 1, 4–7, 10–13, 16, 17, 19–24, 27, 28, 30, 31, and 36–41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pub. No. 2002/01447810 (hereinafter "Traversat") in view of U.S. Pub. No. 2002/0064149 (hereinafter "Elliott"). Applicants respectfully disagree. None of the cited references, alone or in combination, disclose each and every element of the claims.

As shown in Fig. 1 of the present application, an exemplary system embodying aspects of the method of amended claim 1 permits centralized resource access control and permits resource access to be controlled on a more granular level – access to the resource (controlled by the second entity) by the first entity is conditioned upon the properties of a conditional scope expression. (*See* Specification, [0006]; [0029]–[0033]). The properties define levels of access to

a resource based on roles associated with the users as part of an organization model. (See Specification, [0006]; [0029]–[0033]). Advantageously, increasing the granularity of access control allows for "fine-tuning" access to a resource based on roles (e.g., a user with one role may be permitted to only receive data from a resource, while another user with a different role may be permitted to send data to a resource as well as receive data from the resource).

Amended independent claim 1 is directed to a method of providing access control to a resource for one or more users. As specified by the claim, access control is centralized. The method comprises, among other things, receiving at the centralized location an authorization request from a first entity to issue authorization data for the one or more users based on roles associated with the users as part of an organization model. The requests/data are sent to or received from both the first entity and the second entity in the course of providing resource access control from a centralized location. The authorization data includes, among other things, validation information and a "**conditional scope expression** identifying the resource by a resource name and by at least one **property name-property value pair** associated with the resource to conditionally define access to the resource, said **property name-property value pair determining a list of conditions for access to the resource controlled by the second entity**". The method of amended claim 1 further recites elements for validating the authorization data to permit access according to certain conditions, namely, those conditions determined by the property name-property value pair. Claim 1 recites:

receiving at the centralized location a validation request from the second entity to validate **the issued authorization data provided to the second entity by the first entity**;

responsive to the received validation request, validating the issued authorization data based on the validation information included in the authorization data; and

responsive to validating the issued authorization data, sending from the centralized location a response to the second entity indicating a determined validation status, said second entity granting to the first entity access to the resource **according to the conditions determined by the property name-property value pair** when the determined validation status indicates that the authorization data is valid.

Applicants submit the cited art fails to teach or suggest centralized resource access control that permits resource access conditioned upon the properties of a conditional scope expression. According to the Examiner, Traversat discloses the method of claim 1. But the Examiner admits that Traversat fails to disclose sending from the centralized location a response

to the second entity indicating a determined validation status. Instead, the Examiner relies on Elliott as disclosing these elements.

Traversat fails to disclose responsive steps where requests/data are sent to or received from both the first entity and the second entity in the course of providing resource access control from a centralized location. Instead, Traversat discloses:

[0162] An access service may be used to validate, distribute, and authenticate a group member's credentials. The access service may define the type of credential used in the message-based protocols used within the peer group. The access service may be used to validate requests made by one peer to another. The peer receiving the request provides the requesting peer's credentials and information about the request being made to the access service to determine if the access is permitted. In one embodiment, not all actions within the peer group need to be checked with the access service, only those actions which only some peers are permitted to use.

(Traversat, [0162]). In other words, Traversat *merely* discloses that a requesting peer communicates a request to another peer, and that peer then communicates with the "access service" to validate the peer's credentials. *Id.* In fact, Traversat *teaches away* from the responsive steps in amended claim 1, as the "access service" in Traversat interacts only with the peer receiving the request, *excluding the requesting peer* from the process. *Id.* As such, Traversat fails to disclose the elements argued by the Examiner.

The Examiner relies on Elliott to disclose sending from the centralized location a response to the second entity indicating a determined validation status, as noted above. According to the Examiner, it would have been obvious to one of ordinary skill in the art at the time of invention to combine the cited references in the suggested manner. Applicants respectfully disagree that Elliott is an analogous art to either Traversat or the subject matter of the present application. Traversat describes a peer-to-peer platform ("P2P") consisting of computing devices acting as peer nodes (*see* Traversat, [0014]; [0027]; Fig. 1B), while Elliott states that:

[0004] According to a broad aspect of a preferred embodiment of the invention, telephone calls, data and other multimedia information is routed through a hybrid network which includes transfer of information across the internet utilizing telephony routing information and internet protocol address information. A telephony order entry procedure captures complete user profile information for a user. This profile information is used by the system throughout the telephony experience for routing, billing, monitoring, reporting and other telephony control functions. Users can manage more aspects of a network than previously possible and control network activities from a central site, while still allowing the operator of the telephone system to maintain quality and routing selection. The hybrid network also contains logic for responding to requests for quality of service and reserving the resources to provide the requested services.

(Elliott, [0004] – "Summary of the Invention"). Elliott is directed to routing and quality of service functions in a hybrid telephony and data network. *Id.* Applicants submit that it would not have been obvious to one skilled in the arts at the time of invention to incorporate features from a hybrid telephony/data network responding to requests for quality of service with a P2P network when designing a method of providing from a central location access control to a resource. Applicants respectfully request a reference citation disclosing or suggesting this combination. Even in combination, however, it is unclear to Applicants how the combined references disclose "responsive to validating the issued authorization data, sending from the centralized location a response to the second entity indicating a determined validation status, said second entity granting to the first entity access to the resource **according to the conditions determined by the property name-property value pair** when the determined validation status indicates that the authorization data is valid" as recited in amended claim 1. The cited portions of Elliott merely disclose providing product and service offerings for "MCI's business customers" (Elliott, [1289]), a user interface for a user to manage profile information and messages (Elliott, [1567]; [1578]), responses from the ISP to external requests (Elliott, [0944]), a remote monitoring capability to determine degraded or broken connections between platforms, server, or more nodes responsible for retrieving messages and delivering message (Elliott, [1296]), a user login page response that contains a token, a scrambled token value, a user ID, and a passcode (Elliott, [1389]), and finally a user interface for permitting DTMF access to an

automated response unit (Elliott, [1579]–[1581]). Applicants respectfully request that the Examiner explain this rejection if the rejection based on Elliott is continued.

The Examiner also argues that Traversat discloses an expression identifying the resource by a resource name and by at least one property associated with the resource to conditionally define access to the resource. As amended, independent claim 1 recites that the authorization data includes, among other things, "a **conditional scope expression** identifying the resource by a **resource name** and by at least one **property name-property value pair** associated with the resource to **conditionally** define access to the resource, **said property name-property value pair determining a list of conditions for access to the resource controlled by the second entity**". Traversat does not disclose the "property name-property value pair" recited in amended claim 1. Instead, the cited portions of Traversat *merely* describe a universal unique identifier ("UUID") naming service to assign an ID to an entity on the P2P network (*see* Traversat, [0072]; [0159]), a resolver service for receiving query messages and determining which resource implementation should receive the message (*see* Traversat, [0331]), and a security structure for ensuring secure transmission of data between peers on the network (*see* Traversat, [0422]–[0426]). Neither of the disclosed services, however, use a "property name-property value" pair to conditionally define access to access to a resource as recited in amended claim 1. Traversat therefore fails to disclose the elements of the claim as argued by the Examiner.

In view of the foregoing, Applicants submit that Traversat and Elliott fail to disclose each and every element of amended independent claim 1 and, thus, claim 1 and its dependent claims 4–7, 10, and 36–41 are allowable for at least the reasons given above.

Amended independent claim 11 is directed to method for validating at a centralized location authorization data to provide conditional access to a resource for one or more users. The method comprises, among other things, receiving at the centralized location an authorization request from a client to issue authorization data for the one or more users based on roles associated with the users. An affiliate server uses the authorization data for allowing the client to **conditionally** access a resource under its control. In response to receiving an authorization request, an authorization token is generated at the centralized location. The authorization token includes, among other things, a header field representing validation information, a source field representing the identity of the user, and a claim field specifying the resource conditionally, "said

claim field including **a conditional scope expression** identifying the resource by a resource name and by at least one **property name-property value pair** associated with the resource to **conditionally define access to the resource**, said property name-property value pair determining a **list of conditions** for access to the resource controlled by the affiliate server".

Applicants submit that Traversat and Elliott fail to disclose the elements argued by the Examiner for the same essential reasons given above for the allowance of amended independent claim 1. For example, amended independent claim 11 recites, among other things, "**receiving at the centralized location** an authorization request **from a client . . . sending** the authorization token from the centralized location **to the client . . . receiving** at the centralized location [] a validation request **from the affiliate server . . . sending** from the centralized location a response **to the affiliate server** indicating the determined validation status . . .", such that requests/data are sent to or received from both the client and the affiliate server in the course of providing resource access control from a central location. Amended independent claim 11 also recites "**a conditional scope expression** identifying the resource by a resource name and by at least one **property name-property value pair** associated with the resource to **conditionally define access to the resource**, said property name-property value pair determining a **list of conditions** for access to the resource controlled by the affiliate server". Instead, Traversat merely discloses an "access service" that interacts only with the peer receiving the request, *excluding the peer requesting access* from the process (*see* Traversat, [0162]) and an UUID naming service and resolver service (*see* Traversat, [0072]; [0159]; [0331]), both of which fail to disclose a "property name-property value pair" to conditionally define access to a resource as recited in amended claim 11. Elliott *merely* discloses a hybrid network for providing routing and quality of service functions in a hybrid telephony and data network (*see* Elliott, [0004]) and fails to cure the deficiencies of Traversat. As a result, Traversat and Elliott fails to disclose each and every element of amended independent claim 11.

In view of the foregoing, Applicants submit that amended independent claim 11 and its dependent claims 12–13, 16–17, and 19–23 are allowable for at least the reasons given above and the rejection of claims 11–13, 16–17, and 19–23 under 35 U.S.C. § 103(a) should be withdrawn.

Amended independent claim 24 is directed to one or more computer-readable media having stored thereon computer-executable components to control access to a resource by one or more users from a centralized location. As recited in amended claim 24, an authorization component issues **to the first entity**, from the centralized location, requested authorization data for the users based on the roles associated with the users. The issued authorization data includes, among other things, "a **conditional scope expression** identifying a resource by a resource name and by at least one **property name-property value pair** associated with the resource, said property name-property value pair determining **a list of conditions** for access to the resource controlled by the second entity", and also includes the validation information. An interface component recited in amended claim 24 is further adapted to receive "a validation request **from the second entity**, said validation request including the authorization data **issued to the first entity**". Amended claim 24 further recites a parser component adapted to retrieve validation information from the received authorization data and a validation component adapted to evaluate the retrieved validation information, "wherein the interface component is further adapted to send a response from the centralized location **to the second entity** indicating a validation status of the received authorization data responsive to said evaluating the retrieved validation information, said second entity granting to the first entity access to the resource according to the conditions determined by the property name-property value pair when the determined validation status indicates that the authorization data is valid." Similar to amended independent claims 1 and 11, embodiments of the components of amended claim 24 advantageously permit centralized resource control where access control can be defined on a more granular level using a conditional scope expression to define levels of access to a resource based on roles associated with the users. (See Specification, [0006]; [0029]–[0033]).

Applicants submit that Traversat and Elliott fail to disclose the elements argued by the Examiner for the same essential reasons given above for the allowance of amended independent claims 1 and 11. For example, nothing in the cited art shows an interface component such that requests/data are sent to or received from both the first and second entity in the course of providing resource access control from a centralized location. And rather than a "**conditional scope expression** identifying a resource by a resource name and by at least one **property name-property value pair** associated with the resource," Traversat discloses an "access service" that interacts only with the peer receiving the request, *excluding the peer requesting access* from the

process (*see* Traversat, [0162]) and an UUID naming service and resolver service (*see* Traversat, [0072]; [0159]; [0331]), both of which fail to disclose a "property name-property value pair" to conditionally define access to a resource as recited in amended claim 24. As explained above, Elliott *merely* discloses a hybrid network for providing routing and quality of service functions in a hybrid telephony and data network (*see* Elliott, [0004]) and fails to cure the deficiencies of Traversat. As a result, Traversat and Elliott fails to disclose each and every element of amended independent claim 24.

In view of the foregoing, Applicants submit that amended independent claim 24 and its dependent claim 27 are allowable for at least the reasons given above and the rejection of claims 24 and 27 under 35 U.S.C. § 103(a) should be withdrawn.

Amended independent claim 28 is directed to an authorization system in a centralized location. Applicants submit that Traversat and Elliott fails to disclose the elements argued by the Examiner for the same essential reasons given above for the allowance of amended independent claims 1, 11, and 24. For example, amended independent claim 28 recites, among other things, "issuing from the centralized location **to the first entity**, responsive to an authorization request **from the first entity**, the authorization data for a user based on a role associated with the user and for validating, in response to a request **from the second entity**, the authorization **data issued to the first entity**", such that requests/data are send to or received from both the first and second entity in the course of providing resource access control from a centralized location. Instead, Traversat merely discloses an "access service" that interacts only with the peer receiving the request, *excluding the peer requesting access* from the process (*see* Traversat, [0162]) and an UUID naming service and resolver service (*see* Traversat, [0072]; [0159]; [0331]), while Elliott *merely* discloses a hybrid network for providing routing and quality of service functions in a hybrid telephony and data network (*see* Elliott, [0004]). As a result, Traversat and Elliott fails to disclose each and every element of amended independent claim 28.

In view of the foregoing, Applicants submit that amended independent claim 24 and its dependent claims 30–31 are allowable for at least the reasons given above and the rejection of claims 24, 30, and 31 under 35 U.S.C. § 103(a) should be withdrawn.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. It is felt that a full and complete response has been made to the Office action and, as such, places the application in condition for allowance. Such allowance is hereby respectfully requested.

Although the art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the claims. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Robert M. Bain/

Robert M. Bain, Reg. No. 36,736
SENNIGER POWERS LLP
100 North Broadway, 17th Floor
St. Louis, Missouri 63102
(314) 231-5400